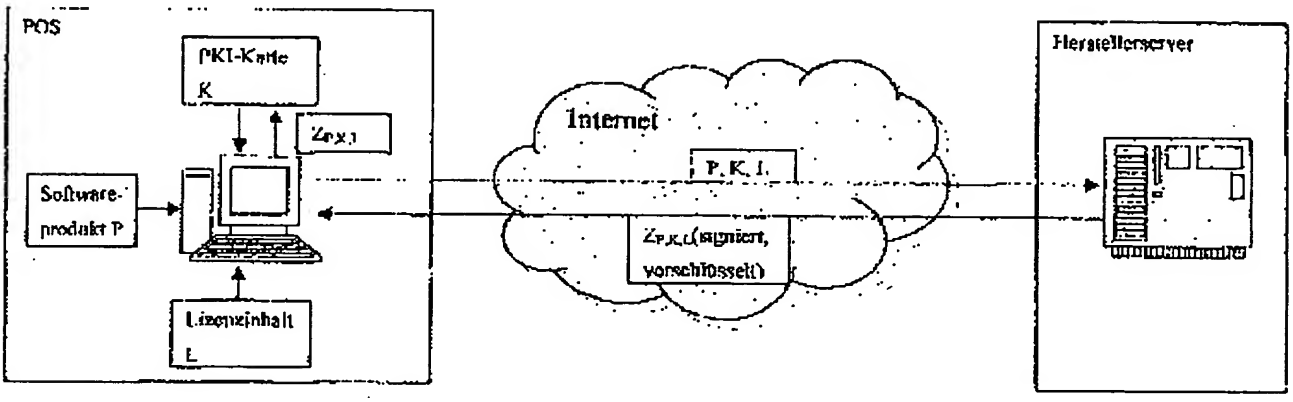
AN: PAT 2003-231356
TI: Preventing misuse of licensed software commercially sold to unknown purchasers involves using purchaser's Public Key Infrastructure card as secure identification, bearer of licensed data
PN: **DE10134356**-A1
PD: 23.01.2003
AB: NOVELTY - The method involves using the purchaser's Public Key Infrastructure or PKI card as secure identification and as a bearer of licensed data combined with the software product to be licensed. The combination is performed purely cryptographically and with software support. Each Internet installation is linked with a manufacturer's server.; USE - For preventing misuse of licensed software commercially sold to unknown purchasers on personal computers. ADVANTAGE - Enables legal transportation of software from one computer to another while withstanding misuse by skilled users with knowledge of internal programs and programming. DESCRIPTION OF DRAWING(S) - The drawing shows a schematic representation of a data flow for the purchase of a certificate (Drawing includes non-English text)
PA: (KLEI/) KLEIN P;
IN: KLEIN P;
FA: **DE10134356**-A1 23.01.2003;
CO: DE;
IC: G06F-012/14;
MC: T01-D01; T01-J20B2A;
DC: T01;
FN: 2003231356.gif
PR: DE1034356 14.07.2001;
FP: 23.01.2003
UP: 04.04.2003



(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 101 34 356 A 1**

(51) Int. Cl.[7]: G 06 F 12/14

(21) Aktenzeichen: 101 34 356.6
(22) Anmeldetag: 14. 7. 2001
(43) Offenlegungstag: 23. 1. 2003

(71) Anmelder:
Klein, Peter, Dr., 63773 Goldbach, DE

(72) Erfinder:
gleich Anmelder

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren zur Verhinderung von missbräuchlicher Verwendung von lizenzierter Software auf Personalcomputern

(57) Die missbräuchliche Mehrfachverwendung von Softwareprodukten, die für Personalcomputer lizenziert wurden, wird über eine kryptographische Anbindung der Produktidentifikation und des Lizenzinhaltes an eine kundeneigene PKI-Karte verhindert sowie über ein dezidiertes Verfahren, das den Lizenzinhaber dazu zwingt, jede Installation und Deinstallation des Produktes inkl. einer hardwaremäßigen Zuorndung auf der PKI-Karte registrieren zu lassen.
Im Gegensatz zu anderen Verfahren vermeidet das erfindungsgemäße Verfahren eine Registrierung des Nutzers beim Herstelle des Softwareproduktes vollständig. Der Nutzer wahrt demnach seine volle Anonymität, und der Hersteller des Softwareproduktes benötigt keinerlei Infrastruktur für die Verwaltung von Nutzerdaten. Das Verfahren ermöglicht hohe Flexibilität bei der Definition der möglichen Lizenzinhalte und erlaubt dem Nutzer insbesondere einen problemlosen Transport seiner Lizenz von einem früheren auf einen neuen Personalcomputer.

DE 101 34 356 A 1

DE 101 34 356 A 1

Beschreibung

1. Wirtschaftlicher Hintergrund, Aufgabe und Lösung des erfindungsgemäßen Verfahrens

[0001] PC-Software für kommerzielle Zwecke, gleich, ob geschäftlicher (z. B. Büroanwendung), technischer (z. B. Datenbanksoftware) oder unterhaltsamer Art (z. B. Computerspiele), wird heute i.d.R. im Handel oder Fachhandel als fertiges Produkt und meistens mit CD-ROMs als Datenträger verkauft. Alle Hersteller von Softwareprodukten klagen über ein hohes Maß an Raubkopien und unberechtigter Nutzung der gekauften Software durch Dritte, denn der Käufer des Softwareprodukte hat ja in aller Regel lediglich eine Nutzungslizenz erworben, die sich zudem nur auf die Installation auf einem Personalcomputer zu einem Zeitpunkt erstreckt.

[0002] Die heute bekannten Lösungen für dieses Problem lassen sich grob in vier Kategorien einteilen:

1. Die auf dem Rechner installierte Software enthält Codestücke, die an sich für den funktionalen Ablauf unwesentlich sind, aber auf den externen Datenträger zugreifen und dessen Vorhandensein und Korrektheit prüfen. Da der sich jeweils nur an einem Ort befinden kann, ist zumindest eine parallele Mehrfachnutzung der Software ausgeschlossen.
2. CD-ROMs als Datenträger werden mit speziellen hardwareorientierten Mitteln gegen kopieren (CD-Brenner) geschützt, z. B. mit Laserlock. Das führt zumindest dazu, dass die Software zu einem Zeitpunkt nur an einer Hardware installiert werden kann. Vor sequenzieller Installation an mehreren Rechnern schützt es natürlich nicht.
3. Für bestimmte Einsatzfälle, besonders im geschäftlichen Umfeld, werden häufig Dongles eingesetzt. In ihrer Funktionsweise gleichen sie stark Methode 1, mit dem Unterschied, dass der Dongle einen geheimen Schlüssel enthält oder auch bestimmte Codestücke, ohne die die zu schützende Software nicht weiter arbeiten kann.
4. In neuerer Zeit wird ein Verfahren eingesetzt, das den Nutzer dazu zwingt, sich bei Benutzung der Software beim Softwarehersteller mit der individuellen Seriennummer der Software (Key-Code) registrieren zu lassen und dabei auch Kennnummern für die eingesetzte Hardware mitzuteilen. Der Zwang erfolgt ähnlich wie bei (1) und (3) Über eingebaute Codestücke, die das Programm bei Nichtregistrierung gewaltsam beenden. Über die Registrierung stellt es der Hersteller fest, wenn ein und die selbe Seriennummer auf mehreren Rechner-Kennnummern eingesetzt werden soll und kann es verhindern.

[0003] Es ist aber bekannt, dass alle diese Wege nur sehr begrenzten Erfolg versprechen. Die Methode 1 wird von Crackern durch relativ kleine Software-Patches unterlaufen, die die kontrollierenden Codestücke der installierten Software (auf der Festplatte) einfach überschreiben. Solche Patches sind leicht im Internet erhältlich und deshalb auch von Nutzern ohne Programmierkenntnisse einfach einzusetzen (besonders bei Jugendlichen für Spiele beliebt). In absehbarer Zeit dürfte auf diese Weise auch Methode 4 konterkariert werden. Methode 4 hat zusätzlich den Nachteil, dass sie von breiten Käuferkreisen wegen des potenziellen Anonymitätsverlustes schlecht akzeptiert wird.

[0004] Methode 2 wird meistens durch verbesserte Kopierprogramme für CD-Brenner unterlaufen. Solche Programme ignorieren die auf den CDs absichtlich eingebauten Fehlerspuren und erstellen ein bitgenaues Abbild des Original-Datenträgers, womit es von diesem nicht mehr unterscheidbar ist.

[0005] Methode 3 ist in bestimmten Fallen wirksamer als Methode 1 (wenn auf dem Dongle notwendige Codestücke des Softwareproduktes abgelegt sind), aber für die Üblichen Anwendungsfälle im kommerziellen und privaten Bereich nicht praktikabel, weil kein Softwarehersteller jeden seiner Kunden mit einem Dongle ausstatten möchte; das wäre viel zu teuer und umständlich.

[0006] Die vorliegende Erfindung schlägt deshalb einen grundsätzlich anderen Weg ein. Als Mittel für Authentifizierung und Kontrolle werden sog. PKI-Karten eingesetzt, die sich aufgrund ihrer anerkannten Sicherheitsstruktur ideal für solche Zwecke eignen. Solche Karten sind heute schon weit verbreitet, und durch neue Anwendungen wie digitale Signatur, Geldkarte, electronic Banking usw. werden sie sich kurzfristig noch stärker durchsetzen. Der Einsatz der PKI-Karte wird kombiniert mit einer nicht umgehbaren Internetanbindung an einen Server des Herstellers bei der Installation des Softwareproduktes. Die Absicherungen erfolgen durch massiven Einsatz von asymmetrischer und symmetrischer Verschlüsselungstechnik, sowohl innerhalb des Softwareproduktes als auch in der PKI-Karte und im Hersteller-Server. Funktional soll mit dem erfindungsgemäßen Verfahren folgende Aufgabe gelöst werden:

- Für ein gegebenes Softwareprodukt auf einem externen Datenträger sollen auf rein elektronischem Weg Lizenzen mit frei wählbaren Lizenzinhalten vergeben werden können; vor allem in Bezug auf parallele und sequenzielle Lauffähigkeit der Software auf verschiedenen Rechnern. Der Nutzer kann sich darauf verlassen, dass er die erworbene Software genauso einsetzen kann, wie es die erworbene Lizenz gestattet. Bei den wählbaren Lizenzinhalten soll insbesondere die Möglichkeit bestehen, Software legal von einem Rechner auf einen anderen zu "transportieren".
- Die eingesetzten Absicherungs- und Authentifizierungsmaßnahmen gegen missbräuchliche Verwendung sollen auch Angriffen von versierten Nutzern mit internen Programm- und Programmierkenntnissen stand halten. Insbesondere sollen diese Maßnahmen die zu schützende Software immun gegen Patches jedweder Art machen.
- Nicht auszuschließende erfolgreiche Angriffe sollen höchstens individuellen Charakter haben, also nicht massenhaft verbreitungsfähig sein, z. B. durch Versenden von Tipps oder Software über das Internet.
- Die volle Anonymität jedes Nutzers soll während der gesamten Nutzungszeit der lizenzierten Software gewahrt bleiben.
- Der Softwarehersteller soll weder gezwungen noch berechtigt sein, seine Nutzer mit ihren Seriennummern o. ä. zu registrieren und zu überwachen; auch eine Kennzeichnung jedes individuellen Produktes (Key-Code) soll überflüssig sein.
- Die Absicherung der Lizenz gegen Missbrauch soll unabhängig von den hardwaremäßigen Eigenschaften des Datenträgers sein, insbesondere unabhängig von dessen etwaiger Kopierfähigkeit.

[0007] Zur Erreichung dieses Ziels werden im wesentlichen folgende Verfahrensschritte und Hilfsmittel eingesetzt:

- Ein Zertifikat für ein Softwareprodukt für einen Nutzer entsteht aus einer datenmäßigen Verknüpfung zwi-

schen der Produktidentifikation und der Identifikation einer nutzereigenen PKI-Karte sowie einem definierten Lizenzinhalt. Die Verknüpfung wird durch eine herstellereigene digitale Signatur zweifelsfrei abgesichert und dadurch zu einem sicheren und nachprüfbaren Zertifikat. Dieser Vorgang läuft beim Kauf über das Internet an der Verkaufsposition (Ladentheke) ab.

- Bei der Erstinstallation wird der Zertifikatsinhalt um eine Identifikation der Hardware ergänzt und auf die PKI-Karte geschrieben. Dies geschieht unter der Voraussetzung, dass die Karte über einen geschützten Bereich verfügt, der nur mit einem herstellerspezifischen Passwort beschrieben werden kann.
- Bei jeder Installation der Software steckt der Nutzer die fürs Zertifikat verwendete PKI-Karte in einen Kartenleser, der an seinen PC angeschlossen ist. Die Installationsprozedur selbst befindet sich nicht oder nur zum kleinen Teil auf dem Datenträger. Statt dessen stellt sie eine Internetverbindung zum Herstellerserver her. Von dort wird sie ganz oder in wesentlichen Teilen heruntergeladen. Dies geschieht jedoch erst, nachdem der Server Zertifikat, Produktidentifikation, Kartenidentifikation und Hardwareidentifikation mit positivem Ergebnis miteinander verglichen hat.

[0008] Das erfindungsgemäße Verfahren benötigt keinerlei Registrierung auf Seiten des Herstellers. Der Server beschränkt sich ausschließlich auf die Kontrolle der empfangenen Daten, eventuell Update und Überspielung der Installationsprozedur bzw. auch Startprozedur an den Nutzer-PC. Deshalb bleibt auch der Nutzer vollkommen anonym, selbst dann, wenn er eine persönliche PKI-Karte o. ä. einsetzt.

2. Definitionen und Voraussetzungen

[0009] Wir legen für die Detailbeschreibungen einige Begriffe fest und identifizieren generelle Voraussetzungen.

[0010] Als intelligente Speicherkarten werden in der Literatur Chipkarten bezeichnet, die sowohl über einen beschreibbaren und wiederbeschreibbaren (nicht flüchtigen) Speicher vertilgen als auch über eigene unveränderliche Identifikation und u. U. zusätzliche Sicherheitslogiken, z. B. die Festlegung von geschützten Speicherbereichen, die nur mit Passwort zugänglich sind. Programmierbarkeit wird für intelligente Speicherkarten in der Regel nicht gefordert. Beispiele für intelligente Speicherkarten sind Telefonkarten, Bankkarten usw.

[0011] PKI-Karten sind intelligente Chipkarten, die zusätzlich mit einem oder mehreren Schlüsselpaaren für asymmetrische Ver- und Entschlüsselungsverfahren ausgestattet sind und natürlich über die Programmlogik verfügen, um Ver- und Entschlüsselungen intern durchzuführen sowie passwortgeschützte Schreib- und Leseaktionen. Wir setzen zusätzlich voraus an, dass unsere PKI-Karten ein spezielles Schreibkommando WRITEPROTECT verstehen, für das der mitgegebene (verschlüsselte) Text zunächst mit dem eigenen privaten Schlüssel entschlüsselt wird, und dann in Abhängigkeit vom mitgelieferten korrekten Passwort eine Schreiboperation ausgeführt wird. Die eindeutige und unveränderliche Identifikation der PKI-Karte nennen wir im folgenden K.

[0012] Die Fälschungs- und Kopiersicherheit von Chipkarten sind Grundvoraussetzungen für alle nachfolgenden Ausführungen. Dies bezieht sich sowohl auf Geheimhaltung bzw. Unveränderlichkeit von privaten und öffentlichen Schlüsseln als auch auf die Echtheit aller durchgeführten Funktionen auf den Speichern und mit dem Betriebssystem der Karte.

[0013] Unter einem Softwareprodukt P verstehen wir ein als wirtschaftliche Einheit am Markt angebotenes Programmsystem auf einem Datenträger (meistens eine CD-ROM), dessen Nutzung der Hersteller dem Käufer entsprechend einem vereinbarten Lizenzinhalt gestatten will.

[0014] Der Lizenzinhalt L beschreibt im einzelnen, zu was der Lizenzinhaber bzgl. des Softwareproduktes berechtigt ist. Wir geben zwei Beispiele:

1. Der häufigste Lizenzinhalt ist die Erlaubnis, das Softwareprodukt zu einem Zeitpunkt auf genau einem Personalcomputer zu nutzen. Es ist demnach nicht erlaubt, das Produkt gleichzeitig auf zwei Personalcomputern zu installieren. Hingegen ist es meistens erlaubt, dies sequenziell zu tun, d. h. für einen bestimmten Zeitraum auf einem Personalcomputer A zu nutzen, das Produkt dort dann zu deinstallieren und es anschließend auf einem Personalcomputer B zu installieren und zu nutzen. Ebenso ist es erlaubt, das Produkt auf einem neuen Personalcomputer zu nutzen, wenn der alte unbrauchbar wurde. Eine Weiternutzung oder Neuinstallation auf dem alten ist damit aber unzulässig.
2. Ein ebenfalls denkbarer Lizenzinhalt ist die Erlaubnis, das Softwareprodukt auf maximal einer festgelegten Anzahl von frei wählbaren Personalcomputern zu nutzen, sequenziell oder parallel. Sind diese einmal gewählt, können keine anderen mehr gewählt werden, jeder weitere Personalcomputer ist unzulässig.

[0015] Ein Zertifikat $Z_{P,K,L}$ für ein gegebenes Softwareprodukt P, eine gegebene PKI-Karte K und einen gegebenen Lizenzinhalt L ist eine zeichenmäßige Verkettung von P, K und L, die vom Hersteller des Softwareproduktes digital signiert ist.

[0016] Eine Nutzungslizenz für ein gegebenes Softwareprodukt ist schließlich die gleichzeitige Verfügbarkeit einer PKI-Karte und eines Zertifikates, das für das gegebene Softwareprodukt, den zugehörigen Lizenzinhalt und diese PKI-Karte ausgestellt ist.

[0017] Eine Installationsprozedur für ein Softwareprodukt ist ein Programm, das die auf CD-ROM liegende Software des Produktes auf dem Betriebssystem des Zielrechners so ablegt und bekannt macht und integriert, dass sie dort aufgerufen und zum Ablauf gebracht werden kann. Üblicherweise ist die Installationsprozedur ebenfalls auf der CD-ROM abgelegt. Unser Verfahren basiert darauf, dass diese Prozedur ganz oder zu wesentlichen Teilen nur über den Internet-Server des Herstellers zu beziehen ist, also nicht auf der CD-ROM liegt.

[0018] Die Hardwareidentifikation eines Personalcomputers ist eine Kombination von Seriennummern einzelner Hardwarekomponenten, die diesen PC insgesamt eindeutig identifizieren.

[0019] Der Herstellerserver ist ein über Internet erreichbarer Rechner des Softwareproduktherstellers, der bei Installation und Deinstallation die notwendigen Dateien liefert und Kontrollen ausführt. Wir nehmen an, dass der Herstellerserver über einen öffentlichen Schlüssel zur Datenverschlüsselung sowie einen Signaturschlüssel verfügt. Außerdem wird angenommen, dass auf der PKI-Karte für den Hersteller ein Schreibbereich reserviert ist, der zusätzlich passwortgeschützt ist. Das Passwort ist unlesbar auf der PKI-Karte abgelegt und ansonsten nur dem Hersteller bekannt.

[0020] Der POS (Point of Sale) ist der Ort, an dem der Kunde sein Softwareprodukt erwirbt.

3. Verfahrensbeispiel

[0021] Wir erläutern an einem Ausführungsbeispiel, wie eine PKI-Karte in Verbindung mit verschiedenen Verschlüsselungsmethoden zur Absicherung der Lizenz genutzt werden kann. Wir nutzen dabei die PKI-Karte als unfälschbaren Identifikator mit Schlüsselpaar sowie als Datenspeicher, der nur mit Passwortschutz beschrieben werden kann. Es gibt folgende Abläufe:

3.1 Erwerb einer Softwarelizenz

a. Der Kunde nennt am POS das gewünschte Softwareprodukt P und legt seine PKI-Karte K vor.
b. Der POS verfügt über einen internetfähigen Rechner mit Kartenleser. Die PKI-Karte des Kunden wird dort eingeführt, und es wird eine Internetverbindung zum Server des Softwareherstellers hergestellt.
c. Der Server liest die Identifikation K der PKI-Karte aus sowie den öffentlichen Schlüssel von K aus der mitgeteilten Produktidentifikation P, dem gewünschten Lizenzinhalt L und aus K erzeugt er eine Verkettung und signiert diese mit der Herstellersignatur zu einem Zertifikat $Z_{P,K,L}$.
d. $Z_{P,K,L}$ wird zusammen mit dem herstellerspezifischen Kartenpasswort mit dem öffentlichen Schlüssel der PKI-Karte verschlüsselt, an den POS überspielt und mithilfe des WRITEPROTECT-Kommandos direkt auf die PKI-Karte geschrieben.
e. Der Kunde bezahlt für das erhaltene Zertifikat und für die CD-ROM mit der Software und erhält seine PKI-Karte zurück.

[0022] Der Ablauf wird bzgl. der zu übertragenden Daten in **Abb.** 1 illustriert.

3.2 Installation des Softwareproduktes auf dem Rechner des Nutzers

[0023] Aus dem nachfolgend beschriebenen Ablauf geht hervor, dass die Installation des Softwareproduktes nicht ohne eine Anbindung an den Herstellerserver möglich ist. Eine grafische Illustration findet sich in **Abb.** 2.

a. Der Besitzer der PKI-Karte K verfügt an seinem PC über einen Internetanschluss und einen Kartenleser.
b. Er startet eine vorbezeichnete Initialisierungsprozedur für das erworbene Softwareprodukt P und wählt "installieren". Da die Installationsprozedur selbst nicht auf der CD-ROM ist, fragt die Initialisierungsprozedur den Nutzer nach einer Internetverbindung zum Hersteller von P. Wenn die Verbindung nicht zustande kommt, wird der Vorgang abgebrochen.
c. Anderenfalls wird vom Herstellerserver sowohl K als auch das Zertifikat $Z_{P,K,L}$ gelesen. $Z_{P,K,L}$ wird auf Konsistenz geprüft und darauf, ob das darin enthaltene K mit der eingeführten PKI-Karte übereinstimmt. Im negativen Fall wird die Installation abgebrochen, im positiven Fall stellt der Herstellerserver die Hardware-Identifikationsdaten des Nutzer-PCs zusammen.
d. Der Hersteller-Server ermittelt anhand von $Z_{P,K,L}$ (Lizenzinhalt, eventuell schon vorhandene Hardwareidentifikation) und der aktuellen Hardwareidentitikation, ob die gewünschte Installation mit dieser Hardwareidentifikation zu-Bissig ist. Im negativen Fall wird der Vorgang abgebrochen.
e. Anderenfalls wird $Z_{P,K,L}$ um die ermittelte Hardware-Identifikation ergänzt und anschließend signiert. Der Server erzeugt ein Schreibkommando für K, bestehend (a) aus dem signierten $Z_{P,K,L}$, (b) seinem Passwort, (c) Datum und Uhrzeit. Er verschlüsselt das gesamte Schreibkommando mit dem öffentlichen Schlüssel von K und sendet den verschlüsselten Satz zu K.
f. Die PKI-Karte entschlüsselt den erhaltenen Satz mit ihrem privaten Schlüssel und verifiziert das mitgegebene Passwort. Falls es nicht korrekt ist, wird der Vorgang abgebrochen. Anderenfalls legt sie das neue $Z_{P,K,L}$ inkl. Datum und Uhrzeit auf dem vorgesehenen Platz ab.
g. Der Server signiert Teil 1 der Installationsprozedur mit seiner Signatur und übermittelt Teil 1 direkt in den Hauptspeicher des Nutzerrechners.
h. Der Nutzerrechner prüft die Signatur von Teil 1 der Installationsprozedur und führt sie direkt aus. Der Code von Teil 1 enthält u. a. einen standardmäßigen Ver- und Entschlüsselungsalgorithmus, die Generierung eines zufälligen Prozedurschlüssels PS dafür sowie die Verschlüsselung von PS mit dem öffentlichen Schlüssel des Softwareherstellers. Der so verschlüsselte PS wird an den Herstellerserver gesendet. PS wird im Hauptspeicher gehalten, aber nirgendwo abgespeichert.
i. Der Herstellerserver entschlüsselt PS mit seinem privaten Schlüssel und nutzt PS dann zur Verschlüsselung von Teil 2 der Installationsprozedur. Der mit PS verschlüsselte Teil 2 wird an den Nutzer-PC übermittelt.
j. Im Nutzer-PC wird Teil 2 mit PS entschlüsselt und anschließend ausgeführt, d. h. das Softwareprodukt wird installiert. Danach wird die Installationsprozedur gelöscht, ohne sie irgendwohin abzuspeichern. PS wird ebenfalls gelöscht. Die Internetverbindung wird beendet. Das Softwareprodukt ist damit installiert.

3.3 Deinstallation des Softwareproduktes von einem Rechner

[0024] Eine korrekte Deinstallation ist für den Nutzer wichtig, weil er damit die Möglichkeit erhält, seine Software ohne Einschränkung auf einen anderen Personalcomputer zu "transportieren". Auch sie ist ohne Internetanbindung und Aktualisierung des Zertifikates nicht möglich. Die zugehörige Deinstallationsprozedur braucht allerdings nicht vom Herstellerserver heruntergeladen zu werden. Sie befindet sich schon auf dem Datenträger des Softwareproduktes.

a. Der Besitzer der PKI-Karte (Nutzer) verfügt an seinem PC über einen Internetanschluss und einen Kartenleser.
b. Er startet eine vorbezeichnete Initialisierungsprozedur für das erworbene Softwareprodukt und wählt "deinstallieren".
c. Der Nutzer wird aufgefordert, eine Internetverbindung zum Herstellerserver herzustellen. Falls das nicht möglich ist, wird der Vorgang abgebrochen. Anderenfalls wird die Deinstallation durchgeführt und vom Herstellerserver auf Korrektheit und tatsächliche Durchführung geprüft. Ist dies nicht der Fall, wird die Deinstallation nicht auf der PKI-Karte vermerkt.
d. Im positiven Fall liest der Server das aktuelle Zertifikat von der PKI-Karte und stellt die Hardwareidentifikation des aktuellen Rechners zusammen. Falls diese nicht mit einer der Hardwareidentifikationen auf dem Zertifikat übereinstimmt, wird die Deinstallation nicht auf der PKI-Karte vermerkt.
e. Anderenfalls wird die Hardwareidentifikation des

aktuellen Rechners vom Zertifikat entfernt. Das aktualisierte Zertifikat mit der Signatur des Rechners versehen.

f. Der Herstellerserver erzeugt ein WRITEPROTECT-Kommando für die PKI-Karte, bestehend (a) aus dem signierten Zertifikat, (b) seinem Passwort, (c) Datum und Uhrzeit und sendet es zur PKI-Karte.

g. Die PKI-Karte entschlüsselt den erhaltenen Satz mit ihrem privaten Schlüssel, verifiziert das mitgegebene Passwort und legt das neue Zertifikat inkl. Datum und Uhrzeit auf dem vorgesehenen Platz ab. Falls das Passwort nicht korrekt ist, wird der Vorgang abgebrochen. Anderenfalls legt die PKI-Karte das neue Zertifikat auf dem vorgesehenen Bereich ab. Damit ist die korrekte Deinstallation im Zertifikat vermerkt.

4. Arbeitsweise mit der Lizenz und Vorteile für Nutzer und Hersteller

[0025] Wir erläutern anhand verschiedener Fälle, wie Nutzer und Hersteller mit der ausgestellten Lizenz umgehen können. Wir nehmen dazu an, dass der vom Nutzer erworbene Lizenzinhalt dem Beispiel 1 in Kap. 2 entspricht.

[0026] Der Nutzer kann sein Softwareprodukt auf seinem zuerst gewählten Personalcomputer beliebig oft neu installieren (nach Kap. 3.2), mit oder ohne vorherige Deinstallation. Falls er sein Produkt deinstalliert (nach Kap. 3.3), wird das Zertifikat auf den Status beim Kauf zurückgesetzt. Falls das nicht tut (z. B. Neukonfiguration des Personalcomputer), stellt der Internetserver bei der erneuten Installation fest, dass sich die Hardwareidentifikation nicht geändert hat (zulässige Hardwareidentifikation) und erlaubt ebenfalls die Installation.

[0027] Der Nutzer kann sein Produkt beliebig oft auf einen anderen Personalcomputer verschieben. Vor einer Installation auf einem neuen Personalcomputer (nach Kap. 3.2) deinstalliert er sein Produkt auf dem alten Personalcomputer (nach Kap. 3.3). Die Hardwareidentifikation des alten Personalcomputer wird damit gelöscht. Damit ist es auch möglich, zu einem späteren Zeitpunkt wieder auf den alten Personalcomputer umzusteigen.

[0028] Wenn der alte Personalcomputer mit dem installierten Produkt als Ganzes unbrauchbar wird (das Produkt also evtl. nicht mehr deinstalliert werden kann), kann er das Produkt auf einem neuen Personalcomputer installieren. In diesem Fall wird die Hardwareidentifikation des alten Personalcomputer im Zertifikat nicht gelöscht, sondern als unzulässig gekennzeichnet. Dies kann er ebenfalls mehrfach wiederholen. Ein Zurückgehen auf den oder die alten Personalcomputer ist damit allerdings ein für alle Mal ausgeschlossen.

[0029] Der Hersteller hat mit den Aktionen des Nutzers praktisch keinen Verwaltungsaufwand. Der Nutzer ist ihm unbekannt, und er hält auch keinerlei nutzerspezifische Daten, sondern nur sein Herstellerpasswort für alle PKI-Karten sowie die Installationsdaten, außerdem für die Dauer des Vorgangs den vom Nutzer erzeugten Prozedurschlüssel. Deshalb ist das ganze Verfahren für den Hersteller äußerst effizient. Der Nutzer seinerseits kann sich darauf verlassen, dass er vollkommen anonym bleibt.

[0030] Wenn der Hersteller "seinen" Speicherbereich auf der PKI-Karte groß genug wählt (in Absprache mit dem PKI-Kartenhersteller), dann kann er natürlich auch für mehrere Softwareprodukte genutzt werden. Der Hersteller kann damit bei einer Installation oder Deinstallation in idealer Weise feststellen, ob es sich bei dem aktuellen Kunden um einen "sehr guten Kunden" handelt und ihm online bestimmte Angebote machen.

[0031] Das erfindungsgemäße Verfahren ist auch geeignet, die Datenträgerlogistik deutlich flexibler zu gestalten. Da der Code des Softwareproduktes an sich für den Kunden wertlos ist (ohne Zertifikat kann er ihn nicht ablaufen lassen), müssen die Datenträger selbst nicht mehr gesichert werden. Es ist sogar denkbar, dass der Händler vom Softwareprodukthersteller überhaupt keine CD-ROMs mehr bezieht. Statt dessen verfügt er über den Code des Softwareproduktes und kann jedem Kunden seine CD aktuell brennen. Je nach Umsatz des Händlers ist dieses Verfahren u. U. deutlich preiswerter als eine zentral gesteuerte Herstellung und Logistik für die Datenträger.

5. Sicherheitsbetrachtung

[0032] Wir listen mögliche Bedrohungsszenarien auf und erläutern, wie das erfindungsgemäße Verfahren diese Bedrohungen abwehrt. Allgemein ist festzustellen, dass potenzielle Raubkopierer entweder versuchen werden, den Zwang zum Update der PKI-Karte zu umgehen (Lokalisierung), oder versuchen, die auf der PKI-Karte abgespeicherten Daten selbst zu manipulieren, um negative Folgen einer Abfrage zu vermeiden. Auf diese beiden Strategien richtet sich daher unsere Aufmerksamkeit.

(1) Eine eigene Installationsprozedur schreiben

[0033] Raukopierer könnten versuchen, die nicht vorhandene Installationsprozedur selbst zu schreiben und damit das Softwareprodukt zu installieren ohne Update des Zertifikates auf der PKI-Karte. Das ist zwar nicht prinzipiell ausgeschlossen, setzt aber eine intime Kenntnis sowohl des Betriebssystems als auch des Softwareproduktes sowie professionelle Programmierkenntnisse voraus. In der Praxis ist das auf breiterer Basis nicht praktikabel.

(2) Abhören der Installationsprozedur Teil 2 bei der Übertragung über unsichere Leitungen

[0034] Dies ist ein anderer Weg, um an den Code der Installationsprozedur zu gelangen. Die Installationsprozedur Teil 2 wird aber immer verschlüsselt übertragen, mit PS als Schlüssel. Dieser wiederum liegt nur temporär im Hauptspeicher und kann nicht eingesehen werden. Deshalb kann der Code der Installationsprozedur beim Leitungstransport nicht abgehört werden.

(3) Manipulation der Installationsprozedur Teil 1 bei der Übertragung

[0035] Die Installationsprozedur Teil 1 könnte dahin gehend manipuliert werden, dass der zu erzeugende Prozedurschlüssel PS auf der Platte abgelegt wird (damit wäre die Entschlüsselung von Teil 2 machbar). Dies ist jedoch unmöglich, denn die Installationsprozedur ist zwar einsehbar, aber signiert mit der digitalen Signatur des Herstellerservers, deshalb kann sie nicht unbemerkt verändert werden.

(4) Selbst die PKI Karte mit einem neuen Zertifikat beschreiben

[0036] Das ist für den Raubkopierer nicht möglich, es sei denn, er ist im Besitz des herstellerspezifischen Passwortes.

(5) Abhören des herstellerspezifischen Passwortes für die PKI Karte

[0037] Die Schreibkommandos an die PKI-Karte inkl.,

des jeweiligen Passwortes gehen als verschlüsselter Datensatz dort hinein (öffentlicher Schlüssel der PKI-Karte). Deshalb kann (außer dem Hersteller) nur die PKI-Karte das Passwort erkennen.

(6) Einen komplettes Zertifikat aus der PKI Karte auslesen und auf eine andere PKI-Karte kopieren

[0038] Dies ist technisch möglich, aber nutzlos, denn das Zertifikat enthält ja eine untblschbare Identifikation der ersten PKI-Karte, die sich immer von der Identifikation der neuen PKI-Karte unterscheiden wird.

(7) Das Softwareprodukt auf mehreren Rechnern hintereinander installieren, ohne Deinstallation auf den früheren Rechnern

[0039] Dies ist prinzipiell zumindest dann möglich, wenn der vereinbarte Lizenzinhalt besagt, dass das Produkt auf einem neuen Personalcomputer N installiert werden darf, sofern der alte Personalcomputer A zerstört oder unbrauchbar ist (der Herstellerserver kann ja nicht feststellen, ob dies tatsächlich der Fall war). Die Hardwareidentifikation von A wird aber im Zertifikat als unbrauchbar notiert, damit kann eine erneute Installation auf A ein für alle Mal blockiert werden. Andererseits ist aber genau diese Möglichkeit zur Neuinstallation des Softwareproduktes für die meisten Nutzer unverzichtbar, etwa nach einem Systemabsturz oder einer Umkonfiguration. Aus diesem Grund stellt eine mögliche Mehrfachinstallation keine reale Missbrauchsgefahr dar.

Patentansprüche

1. Verfahren für eine Absicherung von kommerziell vertriebenen Softwarelizenzen an anonyme Käufer gegen missbräuchliche Mehrfachverwendung, **dadurch gekennzeichnet**, dass eine PKI-Karte des Käufers als sicherer Identifikator und Träger von Lizenzdaten mit dem zu lizenzierenden Softwareprodukt verknüpft wird, dass die Verknüpfung rein kryptographisch und softwaregestützt arbeitet, dass jede Installation des Softwareproduktes an eine Internetverbindung mit einem Server des Herstellers geknüpft wird, dass von diesem Server Installationsdaten, speziell Hardwareidentifikationsdaten, sicher und unfälschbar auf der PKI-Karte abgelegt werden, und dass damit jede nicht gewünschte Mehrfachinstallation wirksam verhindert werden kann.

2. Verfahren unter Einsatz der PKI-Karte mit einem asymmetrischen Schlüsselpaar und den zugehörigen Standardfunktionen (ver- und entschlüsseln, lesen und schreiben mit/ohne Passwortschutz usw.) nach Anspruch 1, dadurch gekennzeichnet, dass die PKI-Kartensoftware eine spezielle passwortgeschützte Schreibfunktion enthält, die die zu schreibenden Daten inkl. des Passwortes in verschlüsselter Form erhält, diese mit dem privaten Schlüssel entschlüsselt und die Nutzdaten abhängig von der Korrektheit des mitgelieferten Passwortes auf den geschützten Bereich schreibt.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass jedem Schreibbereich auf der PKI-Karte ein spezifisches Passwort und ein spezifischer Softwareproduktthersteller zugewiesen ist, und dass jedes spezifische Passwort außerhalb der PKI-Karte nur dem spezifischen Hersteller bekannt ist.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Kauf des Softwareproduktes aus folgenden Komponenten besteht:

i. Bildung eines Zertifikates durch den Herstellerserver, bestehend aus Identifikationen des gewünschten Softwareproduktes, der PKI-Karte des Kunden und des gewünschten Lizenztyps, das Ganze signiert mit der digitalen Signatur des Herstellers,

ii. Ablage des signiertes Zertifikates auf der PKI-Karte des Käufers mithilfe der passwortgeschützten Schreibfunktion nach Anspruch 2 und

iii. Übergabe von PKI-Karte und Datenträger mit Software an den Käufer.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass der festzulegende Lizenztyp eine klare Aussage darüber enthält, auf wie viel verschiedenen Personalcomputern die Software parallel oder sequenziell eingesetzt werden darf.

6. Verfahren für die Auslieferung der zu lizenzierenden Software auf CD-ROM nach Anspruch 4, dadurch gekennzeichnet, dass die Saftware keine Installationsprozedur oder nur einen kleinen Teil davon enthält. Statt dessen wird die Installationsprozedur vor der Installation des Softwareproduktes über eine Internetverbindung zum Herstellerserver in einem mehrstufigen sicheren Verfahren auf den Nutzer-PC heruntergeladen. Die Stufen sind:

i. Teil 1 der Installationsprozedur wird signiert heruntergeladen und ausgeführt. Teil 1 enthält nur die zufällige Generierung eines symmetrischen Schlüssels, dessen Verschlüsselung mit dem öffentlichen Schlüssel des Herstellerservers sowie die Rücksendung des verschlüsselten Schlüssels an den Herstellerserver.

ii. Teil 2 der Installationsprozedur wird im Herstellerserver mit dem symmetrischen Schlüssel verschlüsselt und an Teil 1 im Nutzer-PC gesendet.

iii. Teil 2 der Installationsprozedur wird im Nutzer-PC mit dem symmetrischen Schlüssel entschlüsselt.

7. Verfahren nach Anspruch 6 unter Verwendung der Hardwareidentifikation des aktuellen Personalcomputers, dadurch gekennzeichnet, dass vor der Ausführung der Installationsprozedur zunächst durch den Herstellerserver diese Hardwareidentifikation festgestellt und nach Anspruch 5 als zulässig erkannt werden muss, und dass im positiven Fall zuerst ein aktualisiertes Zertifikat auf die PKI-Karte geschrieben wird, und zwar mithilfe des herstellerspezifischen Passwortes nach Anspruch 2. Das aktualisierte Zertifikat enthält neben den Informationen nach Anspruch 4 zusätzlich die festgestellte zulässige Hardwareidentifikation.

8. Verfahren nach Ansprüchen 2 und 7, dadurch gekennzeichnet, dass das herstellerspezifische Passwort geheim bleibt, weil es nur in verschlüsselter Form (mit dem öffentlichen Schlüssel der PKI-Karte) an die PKI-Karte übermittelt wird.

9. Verfahren nach den Ansprüchen 6, 7 und 8, dadurch gekennzeichnet, dass die Installationsprozedur nach ihrer Ausführung sofort gelöscht wird, ebenso der zufällig generierte symmetrische Schlüssel, und dass durch die Reihenfolge der Ver- und Entschlüsselungen ausgeschlossen wird, dass der Käufer oder eine andere unautorisierte Person in den Besitz der Installationsprozedur gelangt.

10. Verfahren nach Anspruch 7, dadurch gekennzeichnet, dass der Nutzer in seinem Zertifikat die Hardwareidentifikation löschen lassen kann, indem er eine ordnungsgemäße Deinstallation des Softwareproduktes

durchführt, und dass er damit die Möglichkeit erhält, das Softwareprodukt entsprechend Anspruch 5 mit einer anderen Hardwareidentifikation zu installieren. Bei der Deinstallation stellt der Nutzer eine Internetverbindung zum Herstellerserver her. Nach positiver Prüfung der Deinstallation schreibt der Server ein aktualisiertes Zertifikat auf die PKI-Karte, bei dem die aktuelle Hardwareidentifikation gestrichen ist.

11. Verfahren nach den Ansprüchen 7 und 10, dadurch gekennzeichnet, dass der Herstellerserver unerwünschte Mehrfachinstallationen wirksam verhindern kann, weil er bei jeder Neuinstallation am vorhandenen Zertifikat zweifelsfrei erkennt, ob zuvor korrekt deinstalliert wurde.

12. Verfahren nach den vorhergehenden Ansprüchen, dadurch gekennzeichnet, dass der Nutzer beim Herstellerserver vollständig anonym bleibt und keiner Weise registriert zu werden braucht. Aus diesem Grund benötigt der Herstellerserver auch keinerlei Administration bzgl. der Nutzer, die das in Frage stehende Softwareprodukt gekauft haben bzw. einsetzen. Der Herstellerserver kennt lediglich die herunter zu ladende Software, den Lizenzinhalt, das herstellerspezifische Passwort, das für alle PKI-Karten gleich ist, und die Verschlüsselungsprozedur mit dem symmetrischen Schlüssel nach Anspruch 6.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 101 34 356 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 23. Januar 2003

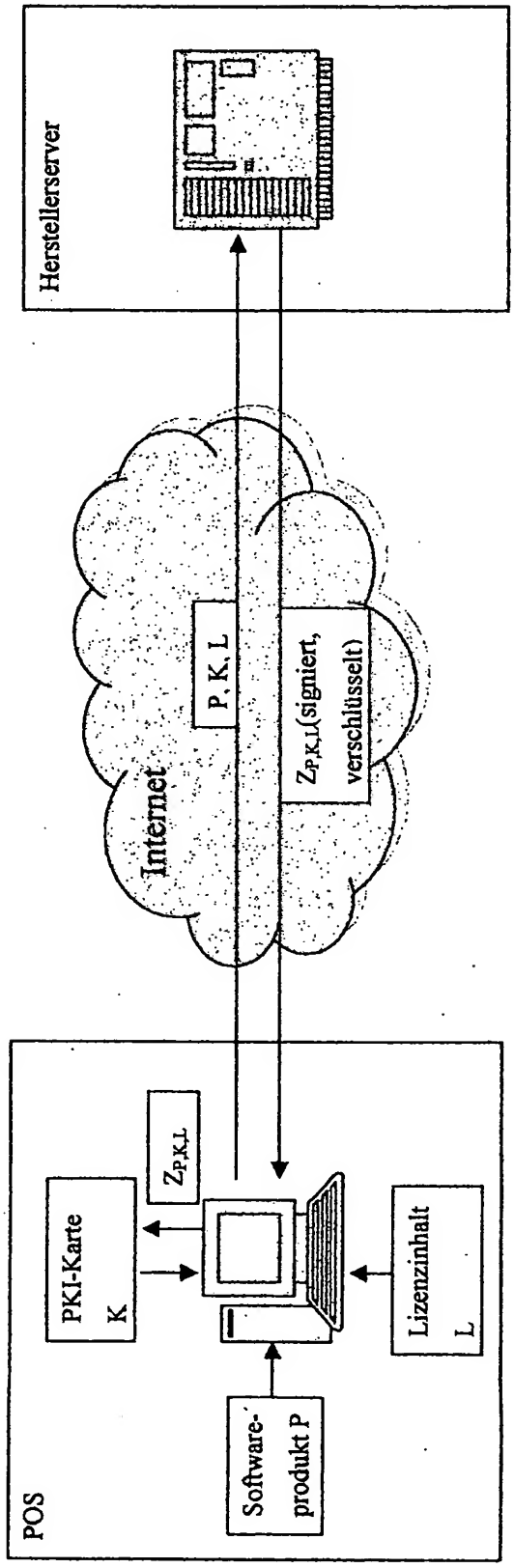


Abbildung 1: Datenflüsse beim Kauf eines Zertifikates

Nummer: DE 101 34 356 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 23. Januar 2003

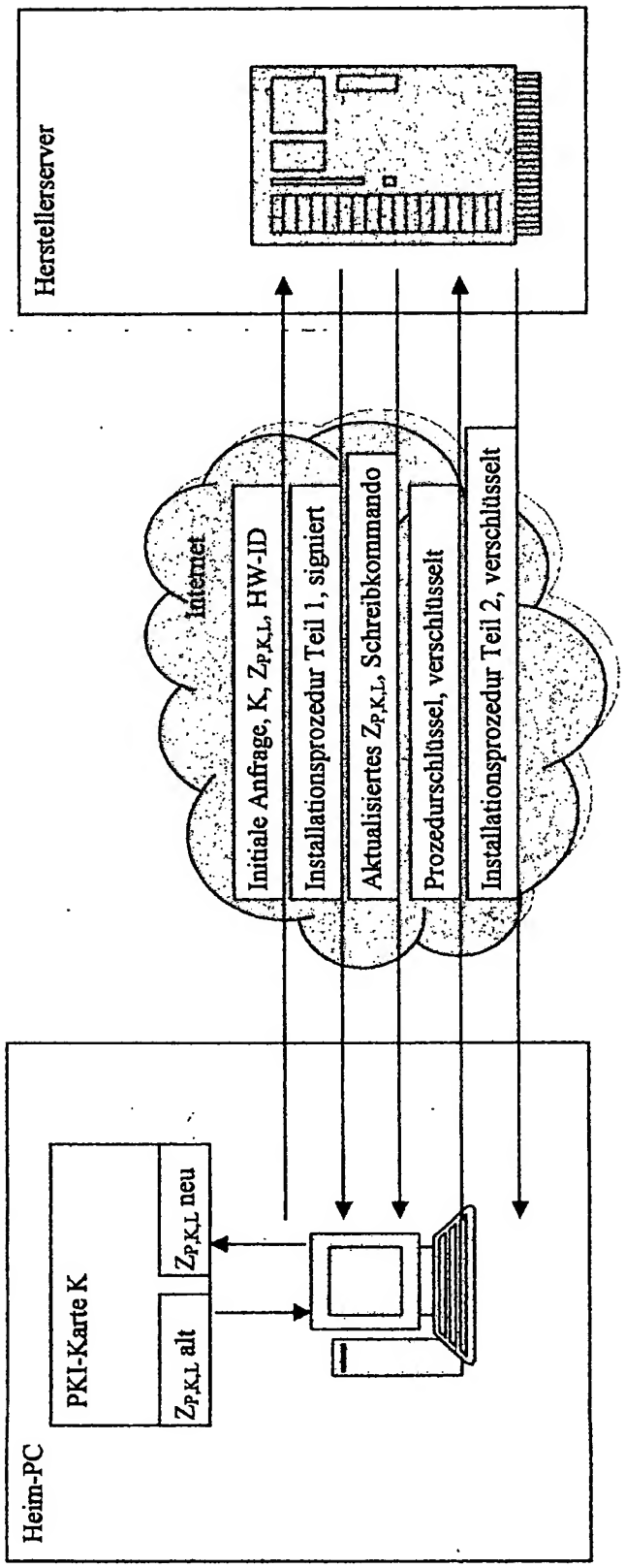


Abbildung 2: Wesentliche Datenflüsse bei der Installation der lizenzierten Software